the called party subaddress and, within this subaddress, several octets can be chosen or defined as a specific location in which that operator ID representative for lawful interception is to be included (see FIG. **1** where five octets are available within the called party subaddress as a specific location).

[0039] Similar annotations as given herein above with reference to FIG. **2** apply likewise to FIG. **3**. The difference is that the called party, i.e. B-party **1***b* is marked to be monitored and it receives a call in the illustrated example scenario. In this regard, MSS-B **2***b* detects a trigger for lawful interception of B-party, responsive thereto composes a setup message to set up a monitoring connection towards the monitoring center as another entity and establishes the monitoring connections towards the monitoring center. Now, in this scenario of FIG. **3**, MSS-B composes the setup message and includes a preconfigured identifier representative for lawful interception into said setup message (message **3** in FIG. **3**), wherein the above-described operator ID is contained in the called party subaddress field, optionally also at a specific location within said subfield, as described above and as illustrated in FIG. **1**.

[0040] Hitherto, the role of the MSS-A and MSS-B (**2***a*, **2***b*) was described with reference to FIGS. **2** and **3**. Now, the functionality of the transit MSS **2***c* shown in FIGS. **2** and **3** will be described. As already derivable from the above description, the transit MSS (e.g. a gateway MSS or the like) represents a network entity equipped with an apparatus comprising a control unit. Such apparatus and its control unit (details see FIG. **4**, for example) are configured to receive a setup message to set up a monitoring connection towards another entity (message **2** from MSS-A **2***a* via transit MSS **2***c* towards monitoring center **3** in FIG. **2** and likewise message **3** in FIG. **3** from MSS-B **2***b* via transit MSS **2***c* towards monitoring center **3**). The transit MSS, i.e. the control unit in the apparatus comprised therein, analyses the received setup message. Responsive to the analysis, the monitoring connection towards said another entity is established and it is further confirmed, based on the analysis, that a preconfigured identifier representative for lawful interception is included with said setup message. Responsive to such confirmation, at least partially a generation of data records for said monitoring connection is suppressed. Namely, based on the detection or verification of the preconfigured operator ID known at the MSS and included in the IAM message (e.g. in the called party subaddress field or a specific octet thereof), CDRs are suppressed from being generated in the transit MSS for the LI (Lawful Interception) traffic only. Thus, the CDRs can be fully suppressed to be generated or at least partially a generation of data records is suppressed in the sense that sensitive information is not contained. Sensitive information in connection with lawful interception means information concerning the intercepted target such as a calling party ID or lawful interception identifier as well as the authority performing lawful interception in the called party. At least this information does not appear in the CDR or not CDR at all is generated, thereby concealing the ongoing interception from the operator in whose network domain the transit MSS is located. Thus, the control unit of the apparatus forming part of the transit MSS is also configured to confirm that the preconfigured identifier is included in a specific message field and optionally to confirm that it is included in a subfield identifying said another entity to which the monitoring connection is established. Optionally, at least it is also confirmed that the preconfigured identifier is included at a specific location within such subfield.

[0041] FIG. **4** shows a basic block circuit diagram of a network entity such as a MSS and/or transit MSS in which embodiments of the present invention are implemented. The MSS as well as the transit MSS, denoted by numeral **4**, comprises a interface, Tx/Rx, cf. numeral **43**, for transmission to/reception from another network entity e.g. another MSS and/or a monitoring center. The interface is bidirectional connected to a control module such as a processor, e.g. a digital signal processor, DSP, or ASIC (ASIC=application specific integrated circuit), CPU (central processing unit), or the like, denoted by numeral **42**. The control module is bidirectional connected to a memory module MEM, denoted by numeral **41**. The memory module can be any type of memory to which data can be written and from which data can be read, e.g. a Flash memory, RAM (Random Access Memory), or also EPROM (Electrically Programmable Read Only Memory). The memory module is configured to store at least the preconfigured operator ID agreed upon to be used for interception. Thus, the memory module can be a separate memory module or a partition of a memory module storing also other user/control data handled by the transit MSS **4**. Other memory modules may be present, too, in the entity. Examples of the invention can be embodied in an apparatus or unit of the transit MSS, e.g. denoted by numeral **40**, comprising at least the modules **42** and **41** above.

[0042] FIG. **5** illustrates an example of a flow chart of a processing performed by a MSS such as MSS-A or MSS-B illustrated in FIGS. **2** and **3**, respectively. The procedure starts in a stage S**50**. In a subsequent stage S**51**, the MSS (an apparatus/control unit thereof) detects an event regarding lawful interception of a calling or called party. Then, in a stage S**52**, an initial address message IAM is composed to be sent towards a monitoring center. In stage S**53**, in such composed IAM, a preconfigured ID for monitoring purpose is included in a specific message field (or optionally also at a specific location within such specific message field) of an initial address message. In a stage S**54**, a monitoring call leg is established towards the monitoring center which includes the lawful interception information such as interception-related information IRI and content of communication from the intercepted target. In a stage S**55**, the procedure related to the present invention in this example then ends.

[0043] FIG. **6** shows an example of a procedure as performed at a transit MSS. As shown in this example scenario, the procedure starts at a transit MSS in a stage S**60**. In a stage S**61**, the transit MSS receives an initial address message IAM from another MSS with a destination to the monitoring center. In a stage S**62**, the transit MSS, i.e. an apparatus or control unit thereof, analyses fields of the IAM. If in a stage S**63** it is found that the IAM does not contain a preconfigured ID for monitoring purposes (NO in S**63**), the flow branches to stage S**64** and charging detail records are generated for the established call leg. If, on the other hand, it is found in stage S**63** that the IAM contains a preconfigured ID for monitoring purposes (YES in S**63**), the flow branches and proceeds to stage S**65**. In stage S**65**, it is checked whether the preconfigured ID for monitoring purposes is present in a specific message field and/or further optionally at a specific location within such message filed. If not (NO in S**65**), the flow can proceed to stage S**64** and CDRs for the established call leg are generated. On the other, if YES in S**65**, it is determined that the IAM pertains to a monitoring call leg and then suppression of CDR generation for the established call leg is performed. This may imply that no CDRs are generated at all, or